UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

KAMILAH JOLLY; DIEGO ALVAREZ-MIRANDA EZPELETA; and VAUGHN BOBB-WILLIS; individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FURTHERED, INC. d/b/a LAWLINE, INC.,

Defendant.

Case No. 1:24-cv-06401-LJL

SECOND AMENDED CLASS ACTION COMPLAINT[1]

DEMAND FOR JURY TRIAL

KAMILAH JOLLY, **DIEGO ALVAREZ-MIRANDA EZPELETA**, and **VAUGHN BOBB-WILLIS**, individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this action for legal and equitable remedies to redress and put a stop to Defendant **FURTHERED, INC. d/b/a LAWLINE, INC.**'s practices of knowingly disclosing Plaintiffs' and its other consumers' identities, their subscription, and the titles of the prerecorded video materials that they requested or obtained, to Meta Platforms, Inc. ("Meta"), formerly known as Facebook, Inc. ("Facebook"), in violation of the federal Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710. [2]

[1] This Amended Class Action Complaint is filed with the consent of opposing counsel pursuant to Federal Rule of Civil Procedure 15(a)(2).

[2] Under the VPPA, 'consumer' means "any renter, purchaser, or consumer of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1).

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its consumers' personally identifying video viewing information to Meta using a snippet of programming code called the "Meta Pixel," which Defendant chose to install and configure on its www.lawline.com website.

3. The information Defendant disclosed (and continues to disclose) to Meta, via the Meta Pixel it installed on its website, includes a consumer's Facebook ID ("FID") coupled with their subscription information and the title of each of the specific videos that the consumer requested or obtained on Defendant's website. A consumer's FID is a unique sequence of numbers linked to the Meta profile belonging to that consumer. The consumer's Meta profile, in turn, publicly identifies the consumer by name (and contains other personally identifying information about the consumer as well). Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals the specific videos that a particular person requested and/or obtained on Defendant's website (hereinafter, "Personal Viewing Information").

4. Defendant disclosed that a consumer purchased a subscription to Defendant's website and its consumers' Personal Viewing Information to Meta without asking for let alone obtaining its consumers' consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information

concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), inter alia, liquidated damages in the amount of $2,500.00 per violation and equitable relief, *see id.* § 2710(c).

6. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiffs bring this Second Amended Class Action Complaint against Defendant for intentionally and unlawfully disclosing their subscriptions and Personal Viewing Information to Meta.

PARTIES

I. Plaintiffs

a. Plaintiff Kamilah Jolly

7. Plaintiff Kamilah Jolly is, and at all relevant times was, a citizen and resident of Orange County, Florida.

8. Plaintiff Jolly has had a Facebook account and has been a user of Meta since approximately 2016.

9. Plaintiff Jolly is a consumer of the video products and services offered on Defendant's lawline.com website. Plaintiff Jolly was a digital subscriber of Lawline from approximately late 2019 to February 2022. She became a subscriber to Defendant's website and Defendant's videos by providing, among other information, her name, address, email address, IP address (which tells Defendant which city and zip code she lives in as well as her physical location), and any cookies associated with her devices.

10. During the relevant time period, Plaintiff Jolly used her Lawline digital subscription to view prerecorded videos and related services through the Lawline website, while logged into her Facebook account. From approximately March 2020 to February 2022, Plaintiff

Jolly viewed videos via Lawline's website. On each such occasion, Defendant disclosed to Meta Plaintiff Jolly's FID, the fact she purchased a subscription, the specific title of the prerecorded video she requested and obtained, and the URL where she requested access to and obtained the video. Defendant also transmitted to Meta information about the device on which Plaintiff Jolly requested and obtained the videos.

11. At all times relevant hereto, including when purchasing a subscription to Defendant's videos and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Jolly had a Meta account, a Meta profile, and an FID associated with such profile.

12. Plaintiff Jolly did not discover that Defendant disclosed her Personal Viewing Information to unauthorized third parties until August 2024, after contacting undersigned counsel and discussing potential claims against Defendant.

13. Plaintiff Jolly never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Personal Viewing Information to Meta. In fact, Defendant has never provided Plaintiff Jolly written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta.

14. Because Defendant disclosed Plaintiff Jolly's Personal Viewing Information (including her FID, her purchase of a subscription, the title of the prerecorded video materials she accessed and obtained from Defendant's website with her paid subscription, and the URL where such video is available to subscribers on Defendant's website) to Meta during the applicable statutory period, Defendant violated Plaintiff Jolly's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

b. Plaintiff Diego Alvarez-Miranda Ezpeleta

15. Plaintiff Alvarez-Miranda Ezpeleta is a citizen and resident of Placer County, California.

16. Plaintiff Alvarez-Miranda Ezpeleta had a Facebook account and was a user of Meta.

17. Plaintiff Alvarez-Miranda Ezpeleta is a consumer of the video products and services offered on Defendant's lawline.com website. He first subscribed to Defendant's website in or about November 2021 and continuously used that subscription to watch videos including on or about September 2022. He maintained his subscription until November 2022. Plaintiff Alvarez-Miranda Ezpeleta became a subscriber to Defendant's website and Defendant's videos by registering for a subscription by providing his name, email address, and zip code.

18. During the relevant time period, Plaintiff Alvarez-Miranda Ezpeleta used his subscription to Defendant's website to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Alvarez-Miranda Ezpeleta's FID, the fact he signed up for a subscription, the specific title of the video he requested and obtained, and the URL where he requested access to and obtained the video. It also transmitted the information about the device he used to request and obtain the video, along with his IP address.

19. At all times relevant hereto, including when registering for a subscription to Defendant's videos and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Alvarez-Miranda Ezpeleta had a Meta account, a Meta profile, and an FID associated with such profile.

20. Plaintiff Alvarez-Miranda Ezpeleta never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact,

Defendant has never provided Plaintiff Alvarez-Miranda Ezpeleta written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta.

21. Because Defendant disclosed Plaintiff Alvarez-Miranda Ezpeleta's Personal Viewing Information (including his FID, his purchase of a subscription, the title of the prerecorded video materials he accessed and obtained from Defendant's website with his paid subscription, and the URL where such video is available to subscribers on Defendant's website) to Meta during the applicable statutory period, Defendant violated Plaintiff Alvarez-Miranda Ezpeleta's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

c. Plaintiff Vaughn Bobb-Willis

22. Plaintiff Bobb-Willis is a citizen and resident of Kings County, New York.

23. Plaintiff Bobb-Willis at all relevant times had a Facebook account and was a user of Meta.

24. Plaintiff Bobb-Willis is a consumer of the prerecorded video products and services offered on Defendant's lawline.com website. He first used Defendant's website in May 2021 to view a course. He signed up for a 1-day trial in September 2023. He then purchased a year-long subscription to Defendant's website in October 2023. Plaintiff Bobb-Willis subscribed to Defendant's website by paying and providing his name, email address, IP address (which tells Defendant which city and zip code he lives in as well as his physical location), and any cookies associated with his devices..

25. On multiple occasions during the two years preceding the filing of this action, Plaintiff Bobb-Willis used his subscription to Defendant's website to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta

Plaintiff Bobb-Willis's FID, the fact he purchased a subscription, the specific title of the prerecorded videos he requested and obtained, and the URL where he requested access to and obtained the video. Defendant also disclosed to Meta information about the device Plaintiff Bobb-Willis used to request the video, along with his IP address.

26. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Bobb-Willis had a Meta account, a Meta profile, and an FID associated with such profile.

27. Plaintiff Bobb-Willis never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact, Defendant has never provided Plaintiff Bobb-Willis with written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta.

28. Because Defendant disclosed Plaintiff Bobb-Willis's Personal Viewing Information (including his FID, his purchase of a subscription, the title of the prerecorded video materials he accessed and obtained from Defendant's website with his paid subscription, and the URL where such video is available to subscribers on Defendant's website) to Meta during the applicable statutory period, Defendant violated Plaintiff Bobb-Willis's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

II. Defendant FurtherEd, Inc. d/b/a/ Lawline, Inc.

29. Defendant is a domestic corporation organized under the laws of New York that maintains its headquarters at 228 Park Ave S., PMB 81742, New York, NY 10003-1502.

30. Defendant operates an online digital library of prerecorded video materials,

including prerecorded video courses, where it is engaged in the business of selling, *inter alia*, a wide variety of prerecorded video materials to consumers across the United States.

JURISDICTION AND VENUE

31. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

32. Personal jurisdiction and venue are proper because Defendant maintains its principal place of business in New York, NY, which is within this judicial District.

VIDEO PRIVACY PROTECTION ACT

33. The VPPA prohibits companies like Defendant from knowingly disclosing to third parties like Facebook information that personally identifies consumers like Plaintiffs as having viewed particular videos or other audio-visual products or services.

34. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business…of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4), and defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3)

35. The VPPA's purpose is as relevant today as it was at the time of its enactment over 35 years ago. Leading up to the statute's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others

personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials, because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

36. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature of such information, and the need to protect it from disclosure, that is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

37. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of

Americans' information."[3]

38. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[4]

39. In this case, however, Defendant deprived Plaintiffs and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

FACTUAL BACKGROUND

I. Defendant Uses the Meta Pixel to Systematically Disclose its Consumers' Personal Viewing Information to Meta

40. As alleged below, when a consumer purchases a subscription to Defendant's website, that purchase of the subscription is communicated to Meta by way of the Meta Pixel. Also, when a consumer requests or obtains a specific video from Defendant's website, the Meta Pixel technology that Defendant intentionally installed on its website transmits the consumer's personally identifying information and detailed information concerning the specific interactions the consumer takes on its website (including the consumer's Personal Viewing Information

[3] *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[4] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, frank.senate.gov (Jan. 31, 2012).

revealing the specific videos that he or she requested and/or obtained) to Meta. All these transmissions are without the consumer's consent, in clear violation of the VPPA.

A. The Meta Pixel

41. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta."[5] Since then, Meta has become the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birthdate, gender, and phone number or email.

42. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to allow them to track consumers' actions and report the actions back to Meta.

43. The Meta Pixel allows online companies like Defendant to build detailed profiles about their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

44. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."[6] Meta is able to do this because it has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[7] – and because each transmission of information made from a company's website to Meta via the

---

5 Company Info, FACEBOOK, https://about.fb.com/company-info./.

6 https://developers.facebook.com/docs/meta-pixel/get-started.

7 For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

45. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

46. Simply put: if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track[] the people and type of actions they take"[8] on the company's website, including the purchases they made, the items they spent time viewing, and, as relevant here, the specific video content that they requested or obtained on the website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Personal Viewing Information of its Consumers to Meta

47. Defendant allows users to become digital consumers of its various online-based video products and services by subscribing to its website or purchasing prerecorded video courses.

48. To subscribe to the Defendant's services or purchase individual video courses, the consumer must provide at least his or her name, email address, billing address, and, if purchasing, credit- or debit-card (or other form of payment) information.

49. After a person has completed the subscription process or gains access to videos

[8] https://www.facebook.com/business/goals/retargeting.

on Defendant's website, Defendant uses—and has used at all relevant times—the Meta Pixel to disclose to Meta the unencrypted FID of the consumer, the purchase of a subscription, and the specific videos that he or she requested or obtained from Defendant's website.

50. Defendant intentionally programmed its website (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its consumers, the fact that a subscription to Defendant's video service was made, and the specific titles of video products that each of them requested and/or obtained in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

51. With only a person's FID and the video content name or URL that the person requested on Defendant's website—both of which Defendant knowingly provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the specific video products or services that this person requested. This can be accomplished simply by accessing the URL www.facebook.com/[unencrypted FID].

52. Defendant's practices of disclosing consumers' purchases of subscriptions to Defendant's website and the Personal Viewing Information of its consumers to Meta continued unabated for the full duration of the time period relevant to this action. At all times relevant hereto, whenever Plaintiffs or another consumer subscribed to Defendant's website or requested a particular video (by clicking on it) on Defendant's website, Defendant disclosed to Meta that (*inter alia*) the consumer subscribed or purchased a subscription and the specific video that was requested or obtained (including the URL where such video was accessed), along with the FID of the consumer who requested it (which, as discussed above, uniquely identifies the person). Specifically, when a user clicked on a video title, added it to cart, initiated checkout, and

purchased the video, Defendant transmitted to Meta through the Meta Pixel, the user's FID, the title and URL of the video requested or obtained, and the action the user took on the website (e.g., "add to cart" or "initiate checkout") at each of those steps.

53. For instance, as shown in the screenshots below, when a user navigates to the website and requests or views a video, Defendant discloses the Personal Viewing Information to Facebook.

Figures 1, 2 & 3: Examples of a HTTP single communication session sent from the customer's device to Facebook that reveals the fact that the user has requested and is viewing the online video "Exploring Emerging Trends in Maritime Sanctions," that they paused it in the process of viewing it, and the customer's unique personal identifiers including the FID (c_user field).

Figure 1

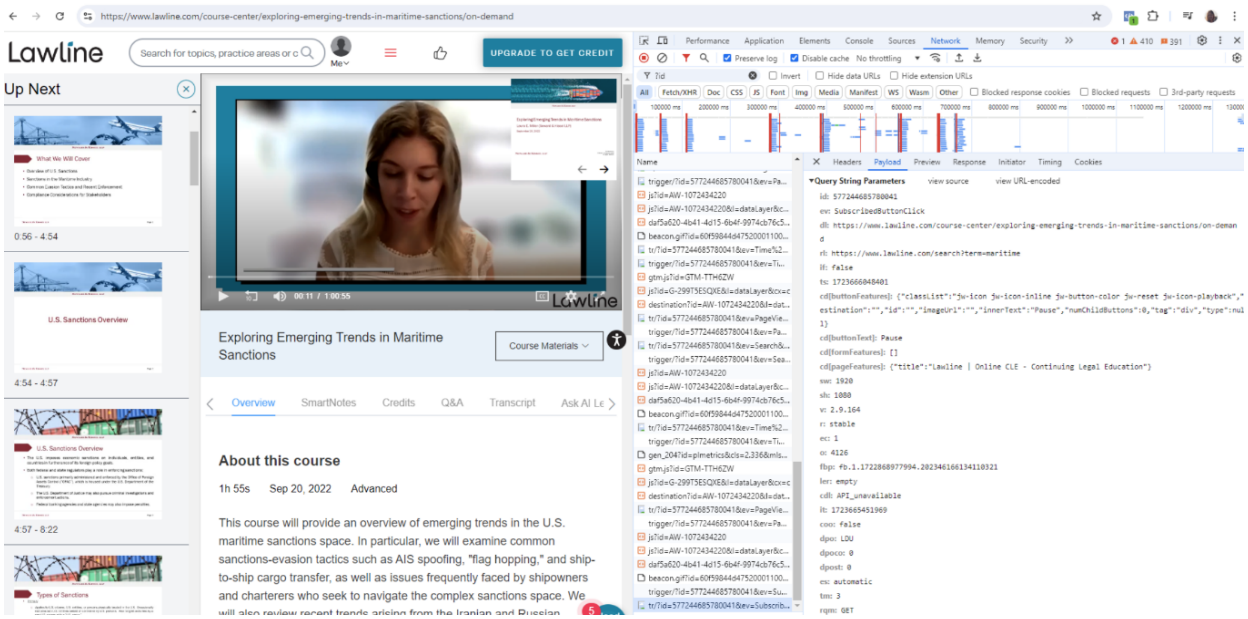
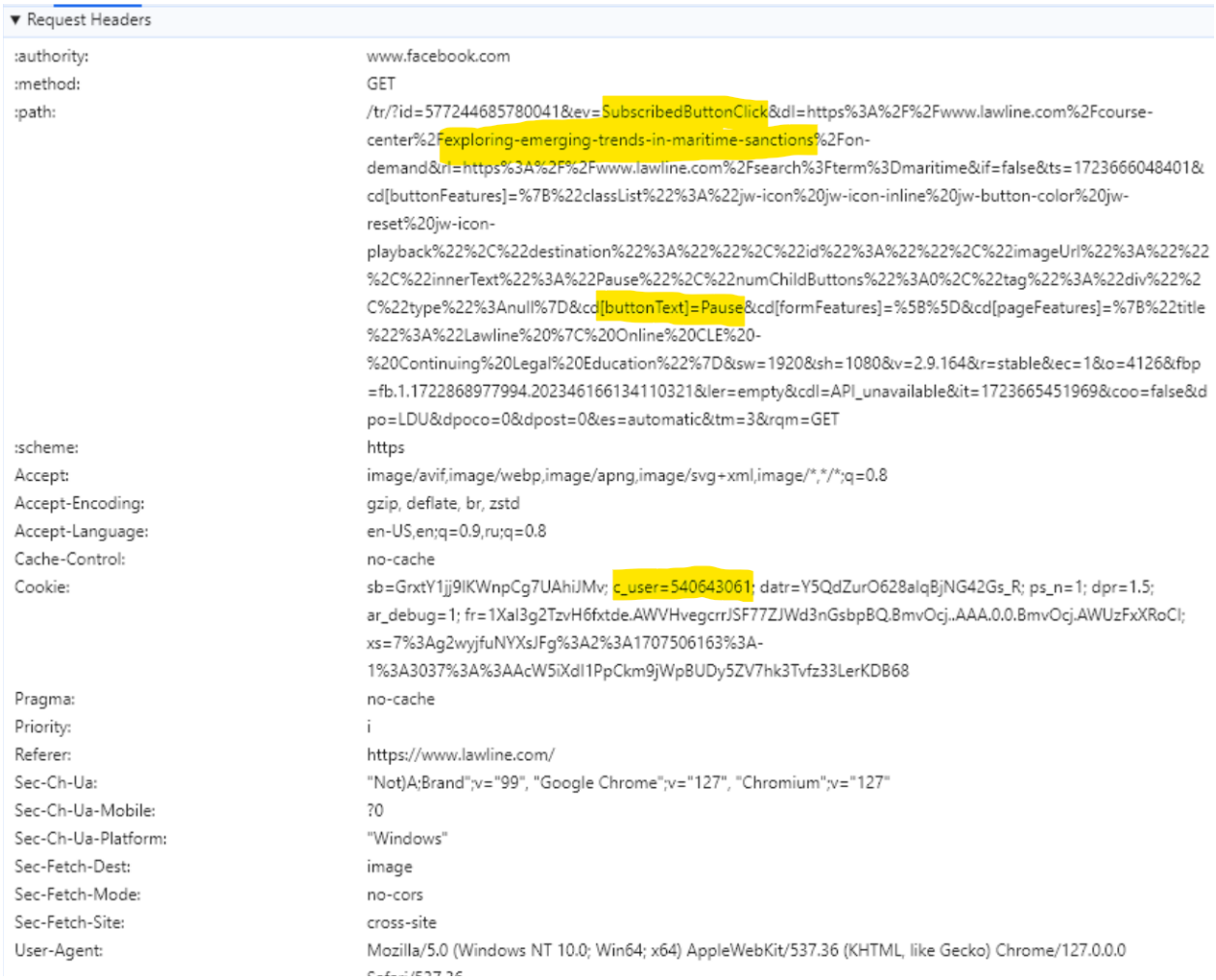


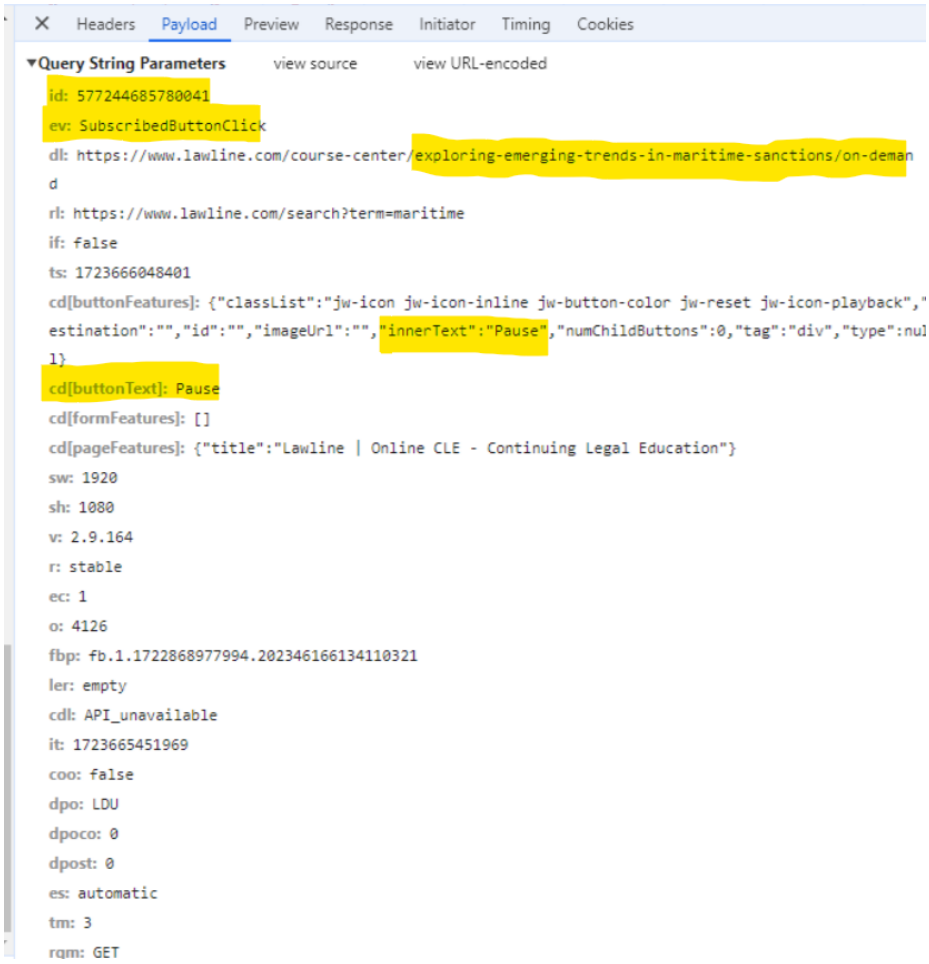
Figure 2



▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/?id=577244685780041&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.lawline.com%2Fcourse-center%2Fexploring-emerging-trends-in-maritime-sanctions%2Fon-demand&rl=https%3A%2F%2Fwww.lawline.com%2Fsearch%3Fterm%3Dmaritime&if=false&ts=1723666048401&cd[buttonFeatures]=%7B%22classList%22%3A%22jw-icon%20jw-icon-inline%20jw-button-color%20jw-reset%20jw-icon-playback%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Pause%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22div%22%2C%22type%22%3Anull%7D&cd[buttonText]=Pause&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Lawline%20%7C%20Online%20CLE%20-%20Continuing%20Legal%20Education%22%7D&sw=1920&sh=1080&v=2.9.164&r=stable&ec=1&o=4126&fbp=fb.1.1722868977994.202346166134110321&ler=empty&cdl=API_unavailable&it=1723665451969&coo=false&dpo=LDU&dpoco=0&dpost=0&es=automatic&tm=3&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br, zstd
Accept-Language:	en-US,en;q=0.9,ru;q=0.8
Cache-Control:	no-cache
Cookie:	sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=540643061; datr=Y5QdZurO628alqBjNG42Gs_R; ps_n=1; dpr=1.5; ar_debug=1; fr=1Xal3g2TzvH6fxtde.AWVHvegcrrJSF77ZJWd3nGsbpBQ.BmvOcj..AAA.0.0.BmvOcj.AWUzFxXRoCI; xs=7%3Ag2wyjfuNYXsJFg%3A2%3A1707506163%3A-1%3A3037%3A%3AAcW5iXdI1PpCkm9jWpBUDy5ZV7hk3Tvfz33LerKDB68
Pragma:	no-cache
Priority:	i
Referer:	https://www.lawline.com/
Sec-Ch-Ua:	"Not)A;Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	image
Sec-Fetch-Mode:	no-cors
Sec-Fetch-Site:	cross-site
User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0

Figure 3



54. Lawline configured its Meta Pixel to transmit to Facebook the URL of the page a customer is navigating which contains the names of the specific videos those customers have requested or obtained. For example, in the screenshots above, Lawline discloses the name of the video (which is synonymous with the name of the course): "Exploring Emerging Trends in Maritime Sanctions."

55. In addition, as illustrated in the Figures 2 and 3 above, Lawline also discloses to Facebook when a customer pauses a video through the "SubscribedButtonClick" event, revealing that the customer has not only requested or obtained that specific video but also that the customer

is viewing the video and has paused the video they are viewing.

56. Lawline also discloses, through a Facebook event named "Time on Page 10 Sec", information regarding how long a user is on the webpage that plays the online video content.

57. At all relevant times, Defendant knew that the Meta Pixel disclosed its consumers' subscription purchases and Personal Viewing Information to Meta.

58. Critically, the Personal Viewing Information Defendant discloses to Facebook allows third parties, like Facebook, to build from scratch or cross-reference and add to the data it already has in their own detailed profiles for its own users, adding to its trove of personally identifiable data.

59. As a result of Lawline's data compiling and sharing practices, Defendant has knowingly disclosed to Facebook for its own profit the Personal Viewing Information of Defendant's consumers including digital subscribers, together with additional sensitive personal information.

60. Defendant could easily have programmed its website so that none of its consumers' subscription purchases or Personal Viewing Information is disclosed to Meta. Instead, Defendant chose to program its website so that all its consumers' detailed Personal Viewing Information is sent to Meta *en masse*.

61. Prior to transmitting its consumers' Personal Viewing Information to Meta, Defendant failed to notify Plaintiffs or any of its other consumers that it would do so, and neither Plaintiffs nor any of its other consumers have consented (in writing or otherwise) to these practices.

62. By intentionally disclosing to Meta Plaintiffs' and Class Members' FIDs together with their subscription purchases and the specific video content they each requested or obtained,

without Plaintiffs' or any of its other consumers' consent to these practices, Defendant knowingly and systematically violated the VPPA on an enormous scale.

II. Consumers' Personal Information Has Real Market Value

63. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[9]

64. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a $26 billion dollar per year online advertising industry in the United States.[10]

65. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[11]

66. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely

---

[9] FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[10] *See Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[11] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

unregulated market.[12]

67. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know [] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[13]

68. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[14]

69. Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[15]

70. Data aggregation is especially troublesome when consumer information is sold

---

[12] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/.

[13] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of- consumer-database-marketing.html.

[14] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

[15] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like NBI share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[16]

71. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[17] The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[18]

72. Indeed, an entire black market exists where the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[19]

---

[16] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[17] *Id.*

[18] *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

[19] *Id.*

73. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

III. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

74. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

75. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies whom they believe do not protect their privacy online.[20] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[21]

76. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors.

77. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[22]

---

[20] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[21] *Id.*

[22] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

78. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[23]

79. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[24] As such, where a business offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a service of less value than the service paid for.

TOLLING, CONCEALMENT & ESTOPPEL

80. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

81. Defendant secretly incorporated the Meta Pixel into its website, providing no indication to customers that their Personal Viewing Information would be disclosed to unauthorized third parties.

82. Defendant had exclusive knowledge that the Meta Pixel was incorporated on its website, yet failed to disclose that fact to its customers, or inform them that by watching videos

---

[23] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

[24] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf ("It is obvious that people value online privacy.").

on the website, Plaintiffs' and Class Members' Personal Viewing Information would be disclosed to third parties, including Facebook.

83. Plaintiffs and other similarly-situated Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the Meta Pixel is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Facebook to intercept its customers' Personal Viewing Information.

84. Defendant had a duty to disclose the nature and significance of its data disclosure practices, including the disclosure of its customers' Personal Viewing Information but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule. Plaintiffs Jolly and Diego did not discover that Defendant disclosed their Personal Viewing Information to unauthorized third parties until August 2024, after contacting undersigned counsel and discussing potential claims against Defendant. Plaintiff Vaugh did not discover that Defendant disclosed his Personal Viewing Information to unauthorized third parties until September 2024, after contacting undersigned counsel and discussing potential claims against Defendant.

CLASS ACTION ALLEGATIONS

85. Plaintiffs seek to represent a class defined as: all persons in the United States who, during the relevant statutory period, requested or obtained a subscription to Defendant's website or video content from Defendant's website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

86. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of

thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

87. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knowingly disclosed Plaintiffs' and Class members' subscription purchases and Personal Viewing Information to Meta; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiffs' and Class members' Personal Viewing Information to Meta; and (d) whether Plaintiffs and Class members are entitled to statutory damages for the aforementioned violations.

88. Plaintiffs' claims are typical of the claims of the Class in that the Plaintiffs and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Personal Viewing Information to Meta.

89. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of Class members.

90. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class Member may lack the resources to

undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In **contrast**, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
(Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710)
(On Behalf of Plaintiffs & the Class)

91. Plaintiffs repeat the allegations asserted in the preceding paragraphs as if fully set forth herein.

92. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

93. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

94. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and Class members, as users who purchased subscriptions to or requested or obtained videos from Defendant's website, are consumers of Defendant's service of providing video content. Thus, Plaintiffs and Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

95. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Defendant knowingly disclosed Plaintiffs' and Class members' Personal Viewing Information to Meta in the manner alleged herein. The Personal Viewing Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiffs and each Class member to Meta as an individual who purchased a subscription or requested or obtained video content, including the specific video materials requested or obtained from Defendant's website.

96. Defendant never obtained informed, written consent from Plaintiffs or any Class member to disclose their Personal Viewing Information to Meta or any other third party. More specifically, Defendant never obtained from Plaintiffs or any Class member informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; Defendant never obtained from Plaintiffs or any Class member informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiffs or any Class member to

withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

97. Defendant knowingly disclosed such information to Meta because Defendant intentionally installed and programmed the Meta Pixel code on its website, knowing that such code would transmit to Meta the subscription purchases and video titles requested by its consumers and its consumers' unique identifiers (including FIDs) when they purchased subscriptions or requested or obtained videos from its website.

98. By disclosing Plaintiffs' and Class members' subscription purchases and Personal Viewing Information, Defendant violated their statutorily protected right to privacy in the videos they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

99. As a result of these violations, Defendant is liable to Plaintiffs and Class members for damages and other relief as provided by the VPPA.

100. On behalf of themselves and all members of the Class, Plaintiffs seek to enjoin Defendant's future disclosures of subscription purchases and its consumers' Personal Viewing Information; liquidated damages in the amount of $2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek a judgment against Defendant **FURTHERED, INC. d/b/a LAWLINE, INC.** as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

B. For an order declaring that Defendant's conduct as described herein violated the VPPA;

C. For an order finding in favor of Plaintiffs and the Class and against Defendant on all counts asserted herein;

D. For an award of $2,500.00 to the Plaintiffs and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c);

E. For an order permanently enjoining Defendant from disclosing the Personal Viewing Information of its consumers to third parties in violation of the VPPA.

F. For prejudgment interest on all amounts awarded; and

G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Class under Rule 23 and 18 U.S.C. § 2710(c).

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury on all causes of action and issues so triable.

Dated: January 29, 2025

Respectfully submitted,

HEDIN LLP

/s/ Julie Holt

JULIE HOLT
HEDIN LLP
1395 BRICKELL AVE., SUITE 610
MIAMI, FLORIDA 33131-3302
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
JHOLT@HEDINLLP.COM

ALMEIDA LAW GROUP LLC

MATTHEW J. LANGLEY
NEW YORK BAR NO. 4831749
DAVID S. ALMEIDA
NEW YORK BAR NO. 3056520

ALMEIDA LAW GROUP LLC
849 W. WEBSTER AVENUE
CHICAGO, ILLINOIS 60614
TELEPHONE: (708) 437-6476
MATT@ALMEIDALAWGROUP.COM
DAVID@ALMEIDALAWGROUP.COM

Attorneys for Plaintiffs and the Putative Class